ABSTRACT OF THE DISCLOSURE

The clocks of remote computing devices are synchronized within a range of certainty through the determination of an upper bound and a lower bound around a reference time. A message from a computing device is propagated up a network tree of devices to a device having a reference time, which encodes the reference time and returns the message down the tree. Each receiving device can determine that the reference time could not have occurred before their transmission of the message, nor could it have occurred after their receipt of the return message. Cryptographic hashes can be used to guard against malicious computing devices. Alternate paths and scheduling of messages can be used to provide a narrower spread between the upper and lower bounds, and clock drift can be accounted for by increasing the spread over time.